

Fort Bend Independent School District

Technology Master Plan Proposal

As of May 1, 2018 - Infrastructure Only

INTRODUCTION AND BACKGROUND

Fort Bend ISD (FBISD) has witnessed a tremendous increase in the use of technology across its environment over the past decade. Technology fills every aspect of our academic and operational environments. Technology can simplify collaboration and communication, empower daily lives, add value to the student experience, and inspire creativity in teaching and learning. In addition, in order for FBISD to realize its mission and vision to our students, these new and increasingly complex technology infrastructures need to be current and reliable for optimal use.

Technologies, while always the “tools” and not the “ends in themselves,” can and will play key roles in the learning environment. The Technology Infrastructure Master Plan is designed to ensure that information technology priorities and initiatives are targeted to support FBISD’s mission and vision. Prioritization and coordination of technology planning and implementation will ensure that FBISD students, teachers, and staff have the combination of skills, knowledge, and technology to succeed in a technology-rich future. A comprehensive and active master plan that focuses on human and financial resources will create the necessary technology infrastructure that provides a technological environment to help “to inspire and equip all students to pursue futures beyond what they can imagine.”

The Technology Infrastructure Master Plan developed in 2014 addressed the state of technology infrastructure in the District based on the recommendations from the work of the FBISD Information Technology Division, the FBISD Technology Steering Committee, Education Partners Solution, Inc., and GoIT. This revised Technology Infrastructure Master Plan identifies and provides recommendation for the remaining technology infrastructure needs.

This plan is developed with the intent to further enhance Fort Bend ISD technology infrastructure to support education, which includes more than simply providing computers and software. As with the previous Technology Infrastructure Master Plan, best practices and industry standards will continue to lay the foundation of this infrastructure plan.

This plan is a working document that will be revised and updated each year. It is flexible with specificity to serve as a guide in decision-making and budgeting. The recommendations contained in this master plan are intended to provide direction for the Board of Trustees, the Superintendent and his Executive Team, principals, teachers, support staff, parents, and students in planning for technology infrastructure projects for the foreseeable future.

I. INFRASTRUCTURE UPDATE:

Bond 2014 provided the necessary funding to address several of the major infrastructure deficiencies Education Partners Solution, Inc., (EPS) assessed in 2014.

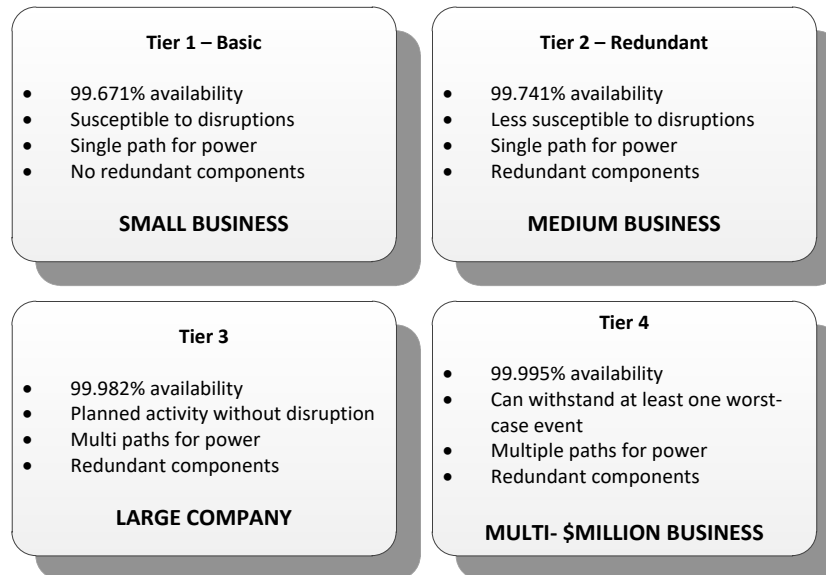
Data Center

Prior to 2014, the District has a single data center located in the Administration Building. The data center is made up of the physical facilities, electrical power, uninterrupted power supplies (UPS), generator, air conditioning, and security to support the District’s comprehensive information and telecommunication systems. The data center serves as the core of the District’s data and voice network, servers, data storage, applications, and Internet for all student and business data and voice services.

The data center was renovated in 2011; however, the EPS report points out that FBISD’s data center is limited to elements of a Tier 1 data center. (See Figure 1) The data center cannot provide mission critical services required to provide reliable, sustainable data and voice needs of the District. The assessment

recommends improvement to the data center infrastructure to increase the level to at least a Tier II which will increase reliability and availability of the data center and its mission critical services.

Figure 1: TIA-942 Telecommunications Infrastructure Standard for Data Centers



With funding from Bond 2014, the data center infrastructure is now a Tier II data center, capable of providing higher availability and redundancy for mission critical applications and network stability. As of the writing of this Technology Infrastructure Master Plan, the Information Technology Division is working on a plan to bring a colocation data center on line. This final phase will provide Fort Bend ISD with an active-active data center solution as recommended by EPS in 2014.

Server Environment

The physical and virtual server environment provides the computation horsepower to run critical applications such as the District’s email system, SharePoint, PeopleSoft, storage, SQL database environments, Kronos, web services, etc. The data center redesign allows for the refresh of all outdated servers. Virtual servers has replaced many old and outdated physical servers, minimizing the data center footprint and associated operational requirements of these physical servers. Key enterprise applications such as Microsoft Office Suite, SharePoint, website, and email are now cloud-based solutions, removed from the reliance of on premise physical servers.

Storage Area Network

The storage area network (SAN) environment stores data, provides storage for backup, and supports the virtual server environment. The re-engineered SAN is optimized with new technologies such as solid state drives, automatic tiering for redundancy, and capacity that handle current storage need, new security camera needs, and future storage requirement.

Cloud storage is an alternative solution that Information Technology Division will examine for long-term storage needs.

An essential component of data management and storage is data backup. Data backup systems were improved significantly to ensure critical business data are backed up to multiple sources to facilitate

resiliency and recovery in the event of a failure. Further enhancements are in progress and anticipated by end of 2018.

Data Network

The data network consists of the wide-area network, the local-area network, and the wireless local-area network. These networks provide the core transport mechanisms for the data and voice traffic from one campus to another campus, to the data center, and/or to the Internet.

1. Wide Area Network

FBISD's wide area network (WAN) provides data and voice connectivity between the District's worksites and campuses to the data center. The re-engineered WAN consists of dual 10 gigabit per second (Gbps)¹, fiber optics network paths from each campus to the data center. The dual fiber connectivity to the data center provides the needed redundancy for data and voice services. The 10 Gbps bandwidth transports the current data requirement with little or no impact on capacity. The re-designed core of the network provides alternate paths to the data center and to the Internet. The new wide area network will be active for the start of 2018-2019 school year.

2. Local Area Network

FBISD's local area network (LAN) provides wired data and voice network connectivity to the classroom. Along with the wireless network, the LAN equipment are upgraded to have the capability to provide 1 Gbps physical network connection to the network device. The project is in its final phase. The last 15 elementary campuses are on the project list for replacement. The LAN project will be completed for the start of 2018-2019 school year.

Another important component of the LAN infrastructure is structured cabling. The upgraded main connections are capable 10 Gbps to allow increased traffic such as wireless and video.

3. Wireless Local Area Network

FBISD's wireless local area network (WLAN) provides wireless connectivity to mobile devices. The WLAN currently provides a standard ubiquitous access wireless network in all upgraded campuses. The project is in its last phase of upgrade with the final 15 elementary campuses' WLAN replaced by the start of 2018-2019 school year. The WLAN project will address the District's administrative buildings and other required coverage areas after the final phase of campus WLAN upgrade.

Internet

Internet access is a critical resource for 24/7 learning and access to digital educational resources for both students and staff. Currently, Internet service is capable of providing 6 Gbps Internet access bandwidth with the capacity of expanding to 10 Gbps if needed. The adoption of "bring your own device" (BYOD) or any other classroom computing device initiative will continue to drive the need for additional bandwidth in the future. An additional 6 Gbps internet circuit will be hosted from the colocation data center and will provide redundancy and resiliency. Efforts are ongoing for the redundancy Internet circuit and anticipated for completion in preparation for the 2018-2019 school year.

Network Access Security

A firewall is a network security device(s) that grants or rejects network access to traffic flows between an untrusted zone (e.g., the Internet) and a trusted zone (e.g., FBISD network). It acts as the demarcation point or "traffic cop" in the network, as all communication should flow through it and it is where traffic is granted or rejected access. It is one of the components of the network that allows the district to be in

¹ Gigabits per second (Gbps) is a data transfer speed measurement for high-speed networks.

compliance with Children Internet Protection Act (CIPA). The firewalls enforce access controls through a positive control model, which states that only traffic defined in the security policy is allowed onto the network; all other traffic is denied.

The district's firewalls have been upgraded with next generation firewalls that facilitate appropriate management of content in a complex environment. The new firewalls provide manageability for applications as well as protection from on-going malicious threats. The configuration and design for these firewalls has followed industry best practice for redundancy and resiliency. Further work effort is in progress to provide additional capabilities to include always on virtual private network (VPN) and multi-site redundancy.

Telephone Network

The existing voice network is a Cisco voice over Internet Protocol (IP) network. The new dual WAN fiber paths from the District's campuses to the data center support the telephone network with higher reliability. The voice system has been upgraded to support the latest features and capabilities afforded by new software version. Further upgrades will be performed as necessary in accordance with district needs as well as to ensure voice system stability and security. The campus staff will continue to have cell phones or analog telephone lines as secondary communication tool.

II. REMAINING INFRASTRUCTURE NEEDS

The 2014 Bond projects addressed many of the major infrastructure deficiencies identified in EPS' 2014 assessment; however, there are many identified infrastructure needs remain.

Local Area Network

The equipment closets that house the network equipment and cabling do not have adequate air conditioning to cool the newly installed equipment. The heat generated by the network equipment in many closets surpasses the vendor's recommended level. Continued overheating will shorten the life of the equipment, resulting in service outage to the classrooms and offices. The immediate need is the upgrade of the air conditioning resources for each equipment closet; however, providing generator power to these closets should also be evaluated to ensure the data and voice services availability during power outage situation.

Access and Security Management

As Fort Bend ISD moves closer to a full digital environment for students and staffs, the needs to maintain strict information security become more prevalent. Access into the FBISD network uses a standard industry authentication process and hardware. This access management system is integrated into Microsoft Active Directory and provides the basic login access for district's devices and applications. The access is not standardized across all applications and devices, leaving users with multiple login processes and procedures. With the advent of a widely deployed WLAN, more mobile devices will be able to login to the network. The ability to integrate and provide a comprehensive identity along with access and a security platform is needed for both the network and applications.

Fort Bend ISD, as many large organizations, has many sources of security event information that exist in different equipment, posing significant delays in stopping or resolving an information security event. In addition to a comprehensive identity management tool, a security information and event management (SIEM) system is needed to provide a tool that assembles all of important digital threat information in a single collection so that priorities and decisions can be made and response times to security events can be minimized. Additionally, a SIEM system can assist in identifying digital patterns that can be used to fine tune response capabilities to provide "proactive" actions against possible system/individual digital compromise.

Management Tools

The district lacks the essential network and server monitoring tools to provide proactive problem resolution and preventive maintenance. Network monitoring tools use server-based system to monitor a computer network for slow or failing components. This system checks components including server-based application, email or web servers, other computing systems and the health of the network itself. These tools are necessary to return network and application services quickly. Management systems will need to be included in information technology toolset.

Telephone

About 7000 of the telephone sets are no longer be supported by the manufacturer since 2015. While cell phones provide the necessary backup, the telephone sets are still used daily and will need to be replaced.

Data Warehouse

FBISD has many disparate sources of data, ranging from student data to human capital resource data and more. Many of the data sources are divided into different data sets that feed into different systems. For example, student data, student achievement data, human resources data, financial data, asset tracking, special education, food services, and professional development feed into different reporting systems. Integrating data from one or more disparate sources creates a central repository of data, a data warehouse.

The data warehouse stores all data in one place where the data are easily accessible. It is essential for the automatic creation of real-time data dashboard that allows the district to operate more effectively and enable teachers and administrators to pinpoint and concentrate on improving certain areas of student achievements.

Fuel Management Hardware Replacement

FBISD's fuel management system has worked well since the implementation of EJ Ward in 2010. Version of software is being upgraded now and this will be complete by June 2018, however, the fuel island hardware terminals are reaching end-of-life in and will no longer be supported by the vendor. FBISD has been notified by the vendor that parts for the aging equipment will become more difficult to procure, so we must plan to upgrade these fuel terminals in 2019. This would impact the existing (3) fuel islands that exist today: Lake Olympia Transportation Center, Hodges Bend Transportation Center, and Police/Facilities location on Murphy Road. Replacement of the fuel management system is a priority.

Timekeeping Clocks

FBISD utilizes Kronos for electronic timekeeping for hourly employees and this has been in place 2005. Today there are 155 original model time clocks installed in various locations throughout the district. Each elementary school has two clocks, one clock for Extended Learning and the other for custodial and cafeteria workers, while each middle and high school each has one clock. Each auxiliary support building throughout the districts has one clock. These clocks have been quite reliable; however, the vendor has informed the district that future firmware will not supported the district's aging clocks. The new clocks were installed in the new elementary schools. They are working well and reliably. An upgrade of all outdated clocks to the latest version of the Kronos clocks is a priority.

III. INFRASTRUCTURE LIFE CYCLE MANAGEMENT

FBISD will develop a life cycle management program to ensure the District's network equipment and servers are up-to-date. Servers and network equipment are generally on a five to seven year replacement cycle with additional servers and network equipment being purchased as the need arises. Core network infrastructure will be on a six to eight year replacement cycle.

FBISD will develop a life cycle management program for computing devices to ensure the District's computing devices remain consistent with current technology.

IV. TECHNOLOGY INFRASTRUCTURE ASSESSMENTS

A Technology Infrastructure Audit will be completed and reported to the Board of Trustees once all Bond 2014 projects are completed. The audit will provide the status of technology infrastructure assessments. These assessments will be necessary to ensure FBISD's technology infrastructure is still viable to support then current technology requirements and needs.

Revised May 1, 2018 2:00 p.m.